

provided for the storage medium in Figure 9, which is discussed on page 19, line 1 through page 23, line 22; and specifically on page 19, lines 14-20 and page 21, lines 15-16 of the present Application.

PRIOR ART

Hasebe #1

Hasebe #1 discloses a data protection system for preventing unauthorized copying of electronic data, such as computer software (Hasebe #1 at abstract, Col. 1, lines 6 - 9). The protected software is provided to the user encrypted on a storage medium such as an optical disk (Col. 1, lines 63 - 65; Col. 2, lines 27 - 29). The electronic key for decrypting the data is stored on the storage medium in encrypted form (Col. 1, line 66 - Col. 2, line 3). The vendor computer supplies encrypted permission information, for decrypting the encrypted electronic data, to the user computer via transmission or to the user in a document (Col. 2, lines 14 - 26). Upon decryption, the unencrypted software is available for execution by the user (Col. 3, lines 37 - 39; Col. 5, line 66 - Col. 6, line 2).

Hasebe #2

Hasebe #2 discloses a system for charging for use of digitized data such as software and for granting permission to use the data (Hasebe #2 at abstract; Col. 1, lines 7 - 9). The supplied data is decrypted for use by a software managing module (Col. 3, lines 46 - 65). Deciphering for subsequent use by the user is permitted only if an available credit balance exists in a charging table (Col. 4, lines 18 - 21). The available balance is subtracted based on the deciphering processing amount or the processing period of time for the ciphered software data (Col. 4, lines 23 - 25). The user can add to the remaining balance total to permit additional use of the data (Col. 4, lines 25 - 29).

Iwayama

Iwayama et al. discloses a system for authorized accessing of encoded electronic data such as computer software (Iwayama et al. at abstract; Col. 2, lines 11 - 15). The data is first stored as encoded data on a storage medium such as a compact disk (Col. 2, lines 30 - 33).

C

The desired portion of encoded data will be decoded when a user inputs the identification information for the preferred data content (Col. 2, lines 61 - 65). When the decoding is completed, the system compares the decoded content identification information with the user-supplied content information (Col. 3, lines 14 - 19). If the two sets of information match, the system will output the selected data portion to the user (Col. 3, lines 19 - 22).

Combination of Hasebe#1, #2 and Iwayama

Combination of Hasebe #1, #2 and Iwayama would be a system incorporating the three systems disclosed in the forgoing references to grant permission for use of electronic data or software. However, the combined system does not disclose preventing during utilization of input data that requires authorization for use certain utilization/processing of the input data (e.g., storage, cut and paste) unless authorization is obtained.

THE PRESENT INVENTION

Regarding the Examiner's comments in item 11 (Remarks) on page 9, lines 1-9 of the Office Action concerning "input data", "data" and "embedding data", the Examiner suggests that the term "embedding" can imply complete integration, such that "input data" and "data", which may include "embedded data" are not distinguishable (i.e., data, including any embedded data, should be treated as the whole data).

However, the present invention uses an approach for creating compound documents (i.e., "linking" or "embedding" of data objects in another data object, another data object being, for example, a document) for preventing use of data without permission, as provided in the description of Figures 2 and 5, on page 13, line 24 through page 14, line 9 of the present Application (*see also*, page 14, line 10 through page 16, line 6).

Therefore, in the present invention a data protection system protects data requiring authorization for use (i.e., input data) against unauthorized use of the data during utilization of the data. Although data requiring authorization for use may be initially authorized for use, for example, by a particular user, subsequent uses of such data may not necessarily be authorized. Therefore, the data protection system according to the present invention prevents such subsequent unauthorized uses by determining whether the data being utilized/processed (for

C

example, the data is being utilized when incorporated in data created by a another user) requires authorization for use. If the data that is being utilized/processed requires authorization for use, the system generates and appends link information in the prepared data specifying the data requiring authorization for use.

In operation, the system judges if the data incorporated in the prepared data requires authorization for use and the system prevents the utilization/processing to be performed on the data requiring authorization for use (e.g., storage, cut and paste) unless authorization is obtained. For example, storage of the original data requiring authorization is forbidden by the system to prevent subsequent unauthorized use of the data. Cut and paste operations on the protected data are also blocked by the present invention. The prepared data may still be utilized/processed without utilizing/processing the data that requires authorization until authorization is obtained.

DISTINCTIONS OF THE PRESENT INVENTION OVER THE PRIOR ART

To further clarify the patentably distinguishing features of the present invention, independent claims 1, 4, 9, 12, 15 and 18-22 are amended, including a new claim 23 is added. Dependent claims are amended to conform to amended independent claims from which the dependent claims depend. Support for the claim amendments can generally be found in Figures 2 and 5; on page 13, line 24 through page 14, line 9; page 14, line 10 through page 16, line 6; and in particular, on page 16, line4-6 of the present Application.

In particular, in contrast to the references relied upon the present invention (as recited in each amended independent claim 1, 12, 22 and new claim 23 (using the recitation of claim 1 as an example) is directed to “a data protection system protecting input data requiring authorization for use against unauthorized use during utilization of the input data”, comprising

- means for creating compound data by linking the input data in data;
- means for “generating information of the input data linked in the data”;
- means for “creating appended compound data by appending the generated information to the compound data”;

C

means for “utilizing the appended compound data by displaying the appended compound data, including displaying the input data linked in the appended compound data”;

judging means for “judging, using the generated information, whether the input data linked in the appended compound data requires authorization for use”; and

means for “preventing storage of the input data linked in the appended compound data in the storage means to prevent unauthorized use of the input data linked in the appended compound data if the input data linked in the appended compound data is judged to require authorization for use”.

A benefit of the patentably distinguishing features is that the system judges if the input data, which requires authorization of use and is in the compound data via linking, requires authorization for use during utilization of the input data (i.e., display of the input data while displaying the compound data) and the system prevents certain utilization/processing (for example, storage, cut and paste or the like as the case may be) to be performed on the input data unless authorization is obtained. Therefore, for example, in the present invention storage of original input data requiring authorization and embedded in data created by a user may be forbidden by the system upon subsequent utilization of the created data to prevent unauthorized use of the embedded input data.

Further, in contrast to the foregoing references, the present invention (as recited in each amended independent claim 4, 9, 15, 20 and 21 using the recitation of claims 4 as an example) comprises

storage means for “storing process information indicating what kind of processing has been performed on the input data in the compound data during the processing”.


A benefit of the patentably distinguishing features is that while information indicating what kind of processing has been performed on the input data in the compound data during the processing can be stored, the original input data that requires authorization for use as well as the original input data after the processing cannot be, for example, stored. Therefore, a user can freely use the information concerning the processing performed on the input data in the

C

compound data but cannot freely handle the original input data in the compound data without authorization for use (*see e.g.*, page 7, lines 3-8; page 22, lines 10-21 of the present Application).

The Examiner in item 4, on page 3, lines 105 of the Office Action asserts that working/preparing means in claims 1, 4, 9, 12 and 15 is disclosed in Hasebe #1. However, Hasebe #1 teaches a data working means for decrypting encrypted data into plain text. However, in contrast to the foregoing references (using the recitation of claims 1 and 22 as an example), the working means (*e.g.*, means for utilization as recited in claim 1 and data display processing unit as recited in claim 22) according to the present invention is means for working plain text, which can be derived or is a result of decrypting encrypted data. Regarding means for generating information relating to input data, the Examiner in item 4, on page 3, lines 6-10 of the Office Action cites portions of Hasebe #2 and Iwayama that relate to means for judging whether the input data should be decrypted or not. In contrast, according to the present invention, information relating to the input data refers to information (LINK information) for causing a display of decrypted input data (*i.e.*, input data after utilization is permitted) in a compound document (*e.g.*, compound data as recited in claims 1 and 22), which incorporates or quotes the decrypted input data. Further, regarding means for updating prepared data (as asserted by the Examiner in item 4, on page 3, lines 15-17 of the Office Action), the prepared data to be updated in claim 12 of Hasebe #2 indicates an update of information for permitting the utilization of the input data. In contrast, according to the present invention, what can be updated is the prepared data (*e.g.*, compound data as recited in claims 1 and 22) containing link information or the like for referring to the input data.

Dependent claims 2-3, (depending, either directly or indirectly, from claim 1), 5-8 (depending either directly or indirectly from claim 4), 10-11 (depending either directly or indirectly from claim 9), 13-14 (depending, either directly or indirectly from claim 12), and 16-17 (depending, either directly or indirectly from claim 15) recite patentably distinguishing features of their own and further are also patentably distinguishing over the foregoing



references at least due to their dependencies from independent amended claims 1, 4, 9, 12, and 15.

For example, claim 10 depending from claim 9 recites “means for distributing the process information from said center as input data requiring authorization for use.” Claim 11 depending from claim 9 recites “means for distributing data prepared by adding the process information to the input data from said center as input data requiring authorization for use.”

The Examiner in item 5, on page 7, lines 3-11 of the Office Action asserts that Figs. 14, 19 and 21 of Iwayama (US Patent No. 5,832,083) (the reference to Hasebe in the Office Action on page 7, lines 8 and 11 being misplaced) suggest the limitation of “means for distributing data”. However, Figs. 14, 19 and 21 of Iwayama are diagrams showing an operation protocol between a utilization permission device and a viewer that uses the decrypted data contents, rather than diagrams explaining a system of data distribution (*see also* Iwayama, Abstract).

Withdrawal of the rejection of claims 1-22, and allowance of claims 1-22 and new claim 23 is respectfully requested.


CONCLUSION

In light of the amendments and remarks presented above, Applicant submits that this Application is now in condition for allowance, and such action is hereby respectfully requested.

C

If there are any formal matters remaining after this response, the Examiner is requested to telephone the undersigned to attend to these matters.

Respectfully submitted,
STAAS & HALSEY LLP

By 
Mehdi Sheikerz
Registration No. 41,307

Date December 4, 2000
700 Eleventh Street, N.W.
Suite 500
Washington, D.C. 20001
(202) 434-1500

C